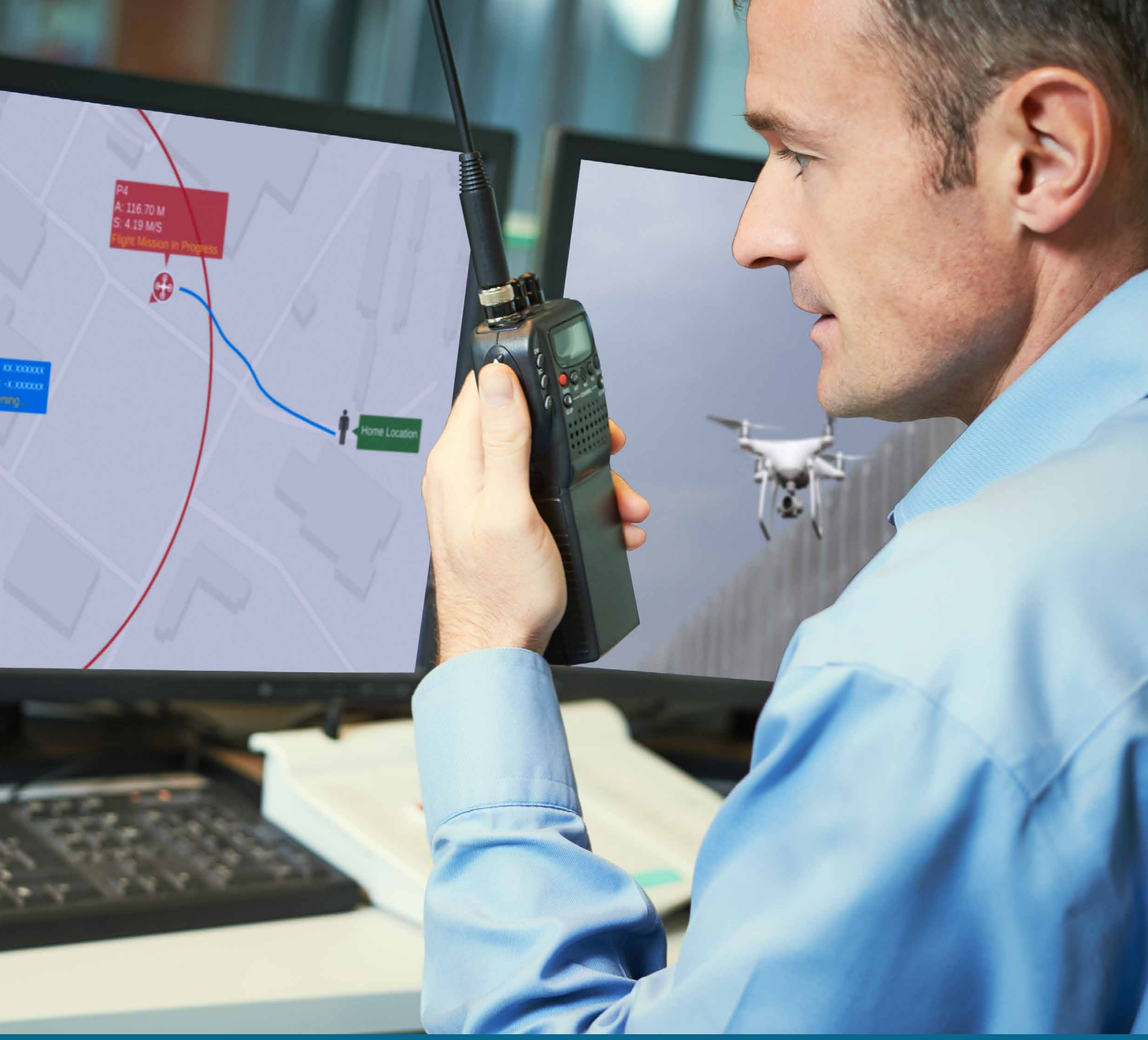


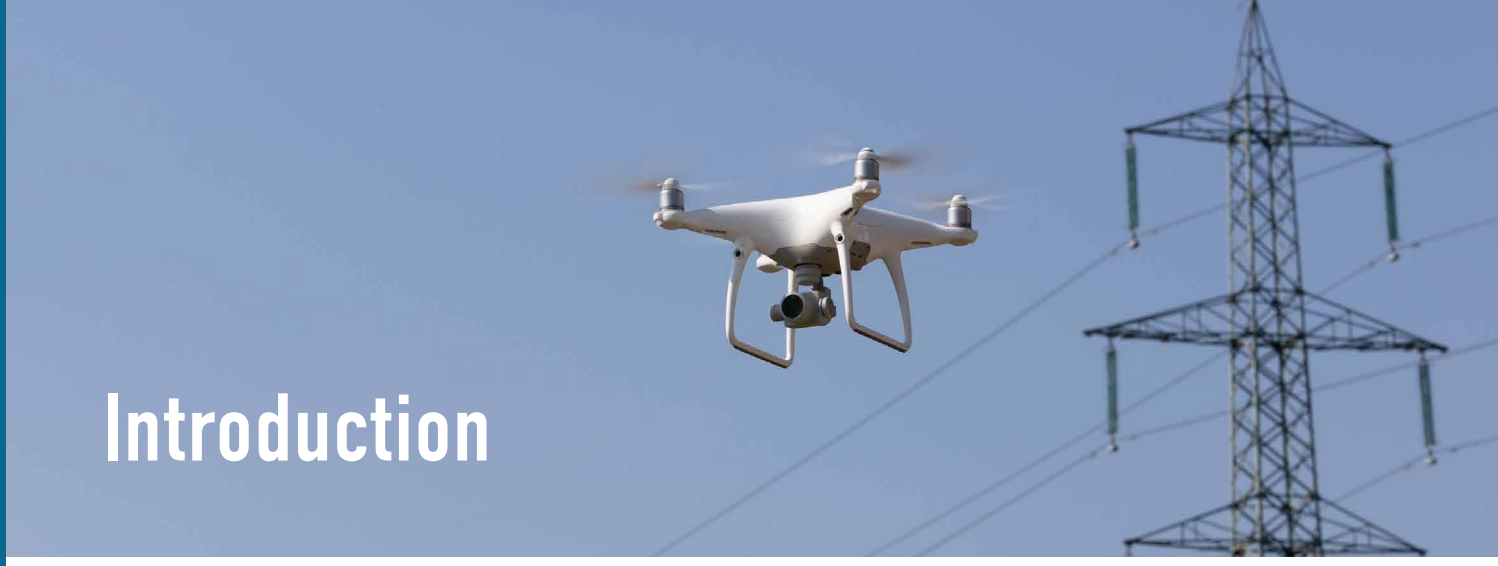
Countering The Threats From Uncrewed Aerial Systems

Developing Operational Requirements for C-UAS Detect, Track and Identify Technology.

Published: April 2023
Classification: Official

National Protective Security Authority

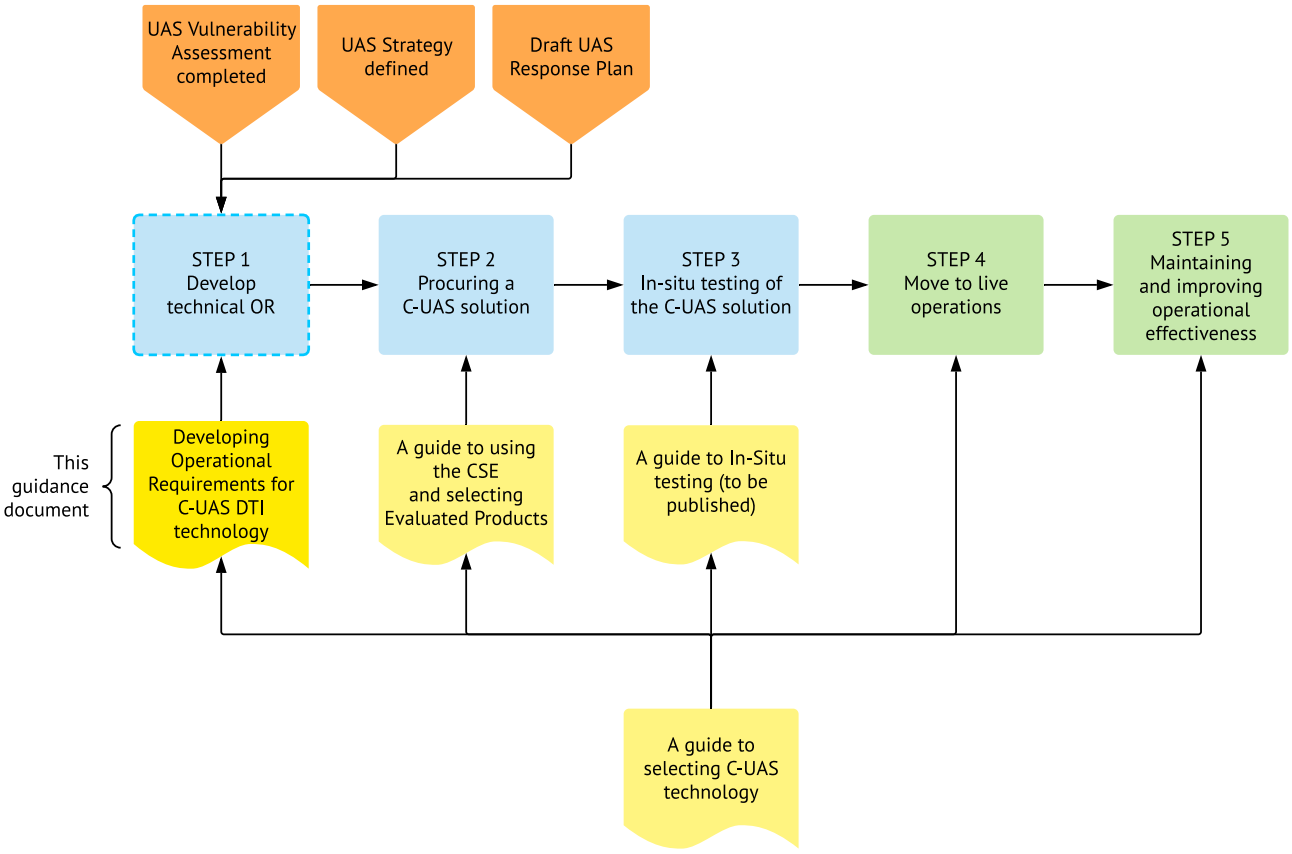
Contents



Introduction

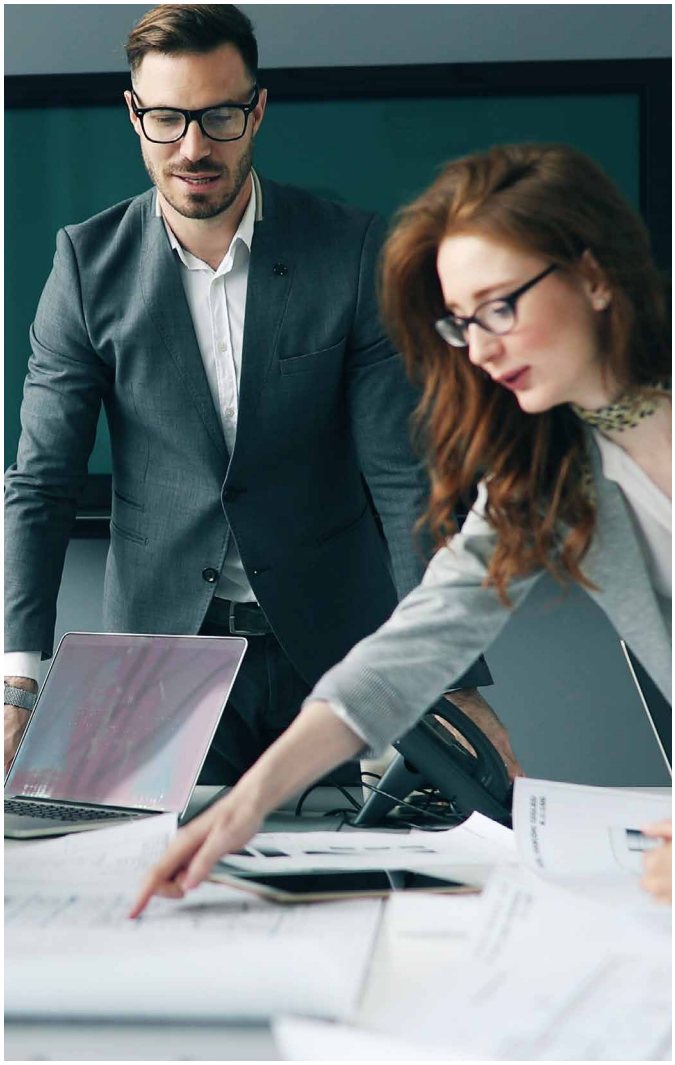
Scope of document

This guidance builds on the framework and guidance set out in the document titled Countering Threats From Uncrewed Aerial Systems – Making Your Site Ready and other supplementary guidance documents, described in Countering Threats From Uncrewed Aerial Systems -guidance document structure. It specifically builds on the information provided in the supplement titled, Countering the threats from Uncrewed Aerial Systems – A guide to selecting C-UAS technology. These documents provide essential pre-reads to this document.



Developing an OR for C-UAS technology is the first of a number of very complex tasks required to successfully deliver C-UAS technology. For this reason sites should only consider developing an OR if they have established that the operational measures already taken are not sufficient and that the residual risk remains unacceptable.

The completed OR will be used to inform the specification process, the procurement of technology and the implementation of an operational solution that will support the mitigation of risk created by the intrusion of Uncrewed Aerial Systems (UAS).

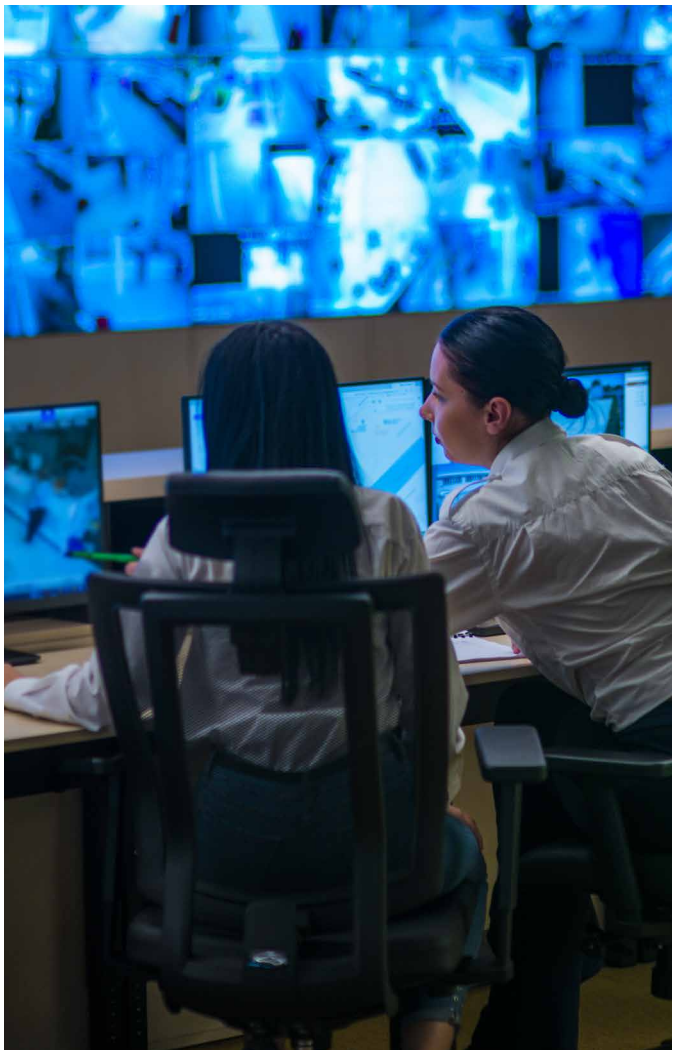


- Site Security Managers
- Physical Security Managers
- Security Control Room Managers
- Business Continuity Managers

The Operational Requirements (OR) Process

The Operational Requirements (OR) process is an approach recommended by NPSA for identifying the requirements of all protective security measures. It is intended to enable an organisation to produce a clear, considered and high-level statement of their security needs based on the risks they face. The OR will inform the selection of the appropriate physical, operational and technical security for all types of security project and, where appropriate, help ensure the effective integration with other systems and operational processes. Developing security measures outside of a structured process often leads to incomplete, inadequate or costly solutions and delays to their delivery.

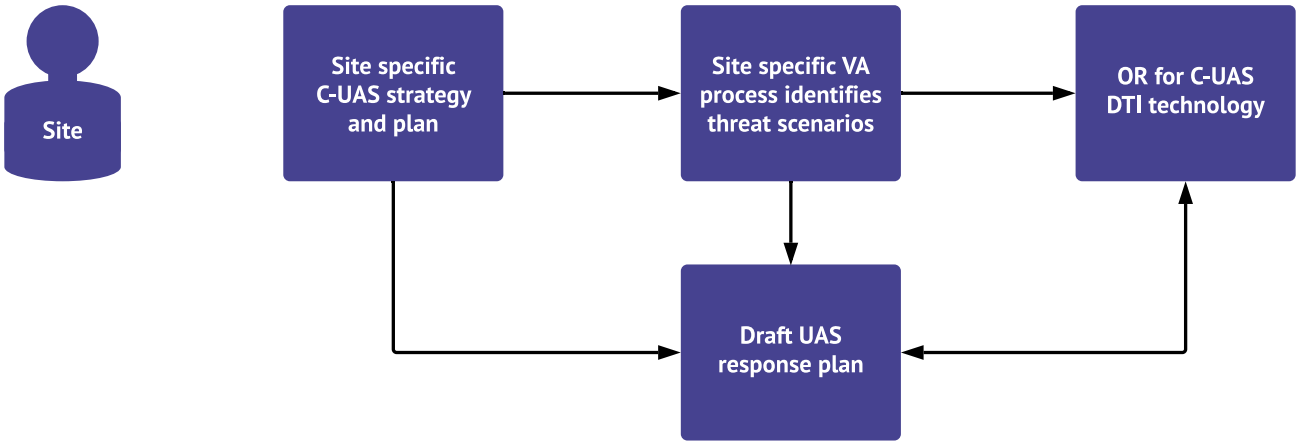
Once a high-level statement of requirement has been produced and agreed, it is necessary to identify the next level of detail. A comprehensive set of requirements needs to be gathered; these will be used to inform the detailed design of the C-UAS technical solution. This document is focused on the creation of this comprehensive set of requirements for C-UAS DTI technology. The process will ensure that all aspects of the C-UAS threat, operating environment, legal and security constraints are considered as a solution is designed, procured and taken into live operation. Following the guidance and answering the questions provided should result in the information gathered being in a format that can be easily understood by those involved in the specification and procurement process.



Information Required To Inform The OR Process

A considerable amount of information will need to be gathered to complete the OR for C-UAS DTI technology. Prior to the development of the OR commencing, it is necessary to ensure that the site-specific products listed below have been completed and are up to date.

- C-UAS strategy
- C-UAS response plan
- UAS Vulnerability Assessment (VA)
- Overall security risk assessment- of UAS scenarios



C-UAS Strategy

When considering if C-UAS technology is required, sites should first create an overarching C-UAS strategy, following the steps identified in the guidance document titled Countering the threats from Uncrewed Aerial Systems – Making Your Site Ready. Only once this has been done, and it has been determined that the risks to the site have still not been adequately mitigated should they consider the use of C-UAS technology. The overarching C-UAS security strategy and associated plan will help determine which internal and external stakeholders to engage with throughout the OR process.

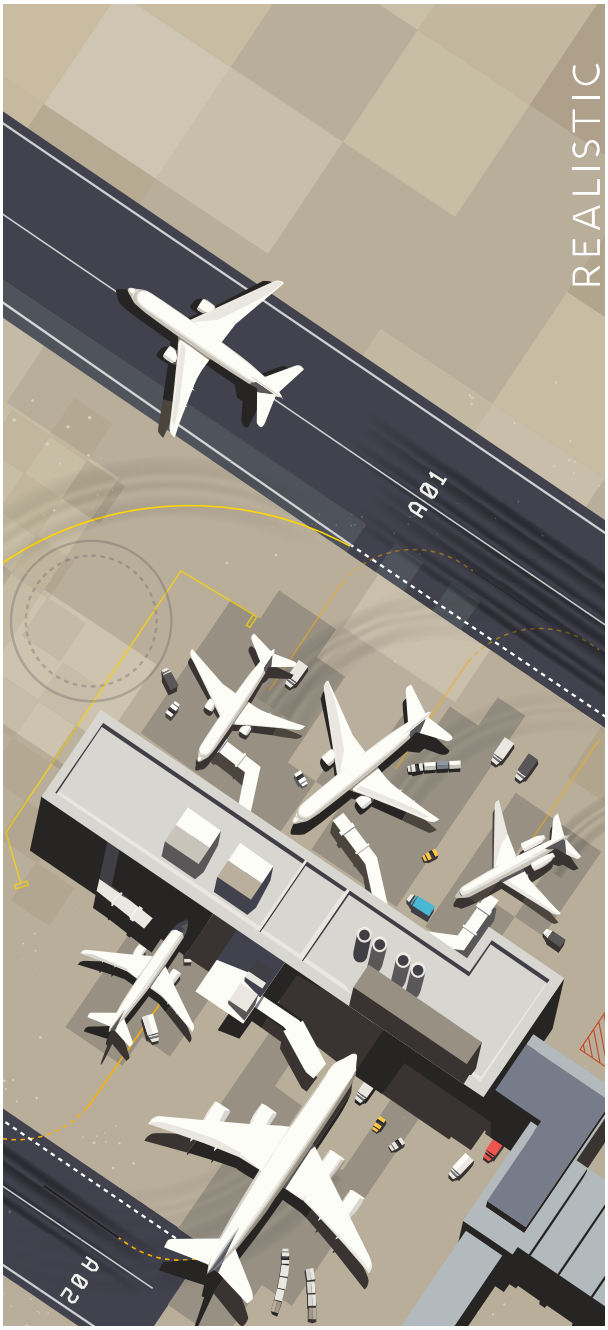
UAS vulnerability assessment

A key step to developing a C-UAS strategy is completing a vulnerability assessment (VA). Detailed guidance on how to carry out a vulnerability assessment is contained within the NPSA guidance document titled: Conducting site vulnerability assessments for Uncrewed Aerial System threats.

The purpose of the VA is to assist those involved in assessing and mitigating the risk to sites from unauthorised UAS activity to identify:

- The key assets vulnerable from a UAS.
- The UAS threat scenarios considered relevant to the site.
- The protection offered by existing mitigations.
- The most likely potential launch sites and flight paths.

The information gathered through the VA process will help inform site specific requirements for C-UAS technology and the associated deployment of this technology (e.g. where should the technology be situated to best counter the threats identified).



Security Risk Assessment

The information from the C-UAS VA will be fed into the site security risk assessment. The risk assessment will score the UAS risks, using the same process as is used to score all other security risks. This will ensure that the UAS risks can be assessed against other security risks, the highest scoring risk are identified and can be prioritised, and that all security risks are dealt with proportionately.

The risk assessment should be used to identify the scenarios that present the highest risk. This information should be used to inform decisions as to which threat scenarios the C-UAS technology should be focused against. It should also be used to ascertain the level of risk that the technology needs to bring down in order to get the associated risks to an acceptable level, and one which is commensurate with other security risks. At a later stage, the risk assessment should be used to identify the level of risk that could be mitigated by the technical measures that are being considered.

C-UAS response plan

There is a critical link between the information delivered by C-UAS technology to a site Security Control Room (SCR) and the operational response that a site is then able to deliver in reaction to a UAS incursion. The information generated by DTI technology will inform the response. The requirements for DTI technology should, therefore, be informed by existing operational response plans and procedures for the site. Once the OR has been completed, and a new technical capability introduced it will be important to make sure the draft response plans and procedures are updated and make the best use of the information that is provided by the new technology. The response plan will form part of the overall C-UAS plan and include:

- How an incident is reported, and as much information as possible is gathered.
- How the information gathered is assessed.
- The response to that incident.

The response plan will be supported by a testing and exercising plan, and a training plan. These plans will help ensure that the plan works and staff are able to deliver what is required of them.

Determining how an incident is reported will assist in understanding what is classed as a confirmed detection, and the role of the C-UAS system in this. Understanding how the information gathered is assessed will assist in identifying what information is required from the DTI system to assist the SCR staff in making an assessment of the threat and determining the response; for example, the number of UAS, the type of UAS, the location of UAS, whether it is carrying a payload, should the police be called and what information should they be provided with. Furthermore, the response plans will assist in determining requirements such as whether tracking capability is required.

The technical solution must recognise how the response will be operationally delivered. It should acknowledge the number of security officers and their ability to deploy both inside and outside the site to search for a pilot, the UAV or both.

The configuration of the SCR may impose constraints on the technology; for example, the number of operators available in the control room may determine the level of engagement that operators will have with the technology. Those with few operators will need a highly automated system.

Developing An OR For C-UAS DTI Technology

Detect, track and identify requirements

The information identified above should be used to inform the development of the OR for C-UAS DTI technology.

The OR will include two types of requirement, namely:

- Generic requirements and
- Site specific requirements.

Generic requirements

The NPSA C-UAS standard specifies generic requirements deemed necessary for use at CNI sites, to ensure integration with the wider protective security strategy and associated security control room response. These requirements provide a base level of capability that should be achieved by every DTI system.

They are intended to ensure that each system:

- Can be controlled and operated from within a SCR.
- Detects representative threats.
- Produces audible and visible alerts that are easily recognised.

Some examples of these generic requirements are:

- The system is commercially available.
- The system is usable by a single operator, following training.
- The system requires minimal operator interaction under normal non-alarm conditions.
- The system is required to have access controls to limit unauthorised usage.
- The system is required to provide DTI information overlaid on a map of site and surrounding area of interest.
- The system provides visual and audible information to the operator on all UAS activity.
- The system records detailed activity logs of UAV detections declared.

The full set of generic requirements are listed in annex A of Countering Threats From Uncrewed Aerial Systems - A guide to using the CSE and Selecting Evaluated Products.

Site specific requirements

Types of requirement

In addition to these defined generic requirements, every site will need to develop a set of site specific requirements.

The site requirements will be divided into a number of different types and will be determined by:

- **The Threat** scenarios that a site needs the DTI to be able to 'detect'.
- **Operational needs** – What information is needed to inform a response? How is the information presented in the SCR and used by security officers as part of the C-UAS response plan? What level of integration is required with other systems?
- **Environmental Requirements** – The environment in which the DTI is to operate (e.g. the geographic location and features, weather, night or day, local activity/equipment whose operation may be interfered with or interfere with the operation of this equipment).
- **Legal considerations** - Ensuring compliance with the legal framework that the equipment provided needs to operate within.
- **Information security** – Responding to the risks associated with data held within the C-UAS technology.

OR questions

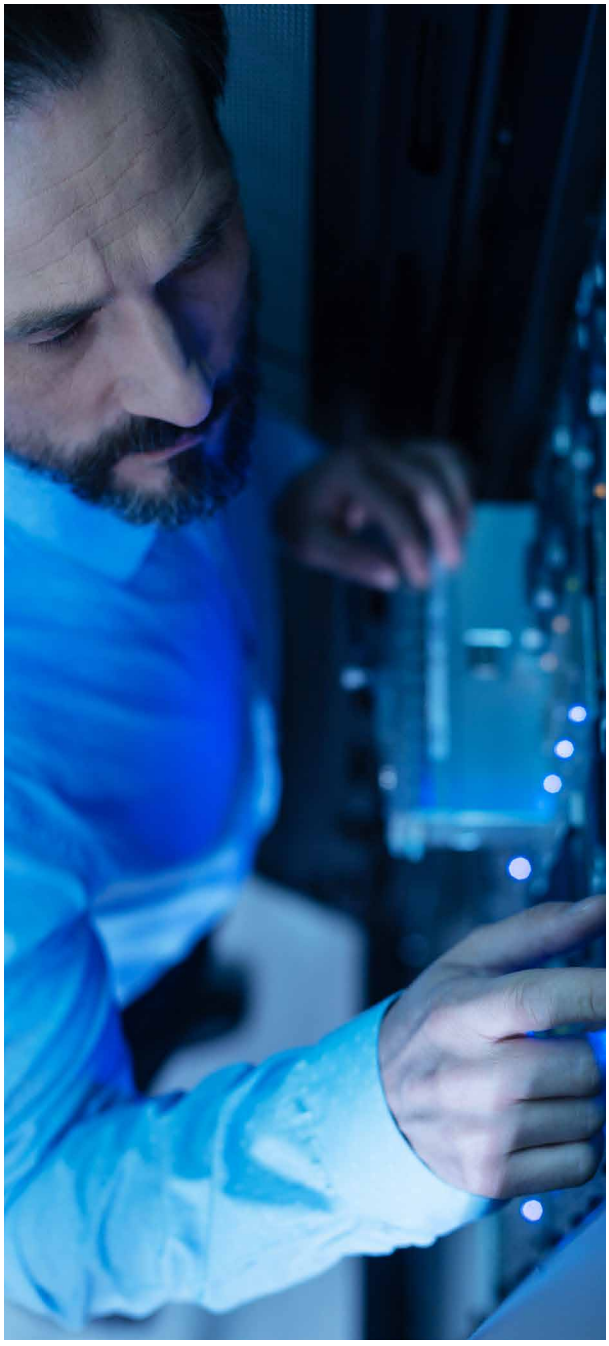
A list of questions is provided at Annex B, to assist with the development of the OR.
The list sets out:

- The questions to be answered
- Where the reader can find information to assist them in answering the question,
- Additional information intended to assist in the development of the answers.

Legal considerations

C-UAS technologies are rapidly developing and their operation may be subject to various laws and regulations which may differ according to the manner of operation of the precise system in question. To ensure compliance with any applicable laws it is recommended that sites seek legal advice as they work through the OR process.

It is the responsibility of the equipment purchaser and the supplier to ensure that any system is suitable for each deployment and that it complies with all legislation, standards, codes of practice and other relevant requirement. Therefore, prior to procurement and deployment detailed guidance should be sought from a site's legal advisers to confirm a system's compliance. Legislation to consider includes, but is not limited to, the Data Protection Act 2018, the Investigatory Powers Act 2016, the Wireless Telegraphy Act 2006 and the Computer Misuse Act 1990.



Security considerations

The nature of C-UAS DTI systems is such that they are intended to handle a wide variety of data that could be sensitive in nature. They may record imagery, video, audio and location data associated with UAS use, and may capture data from other devices operating in the same frequency bands in the surrounding area. In many cases the data gathered may be shared with organisations and in places beyond the control of the C-UAS operator.

There are a number of necessary and legitimate data transmissions that a C-UAS system is likely to make with an external server. For example, the regular updating of the C-UAS software, or the reporting of errors and faults to the manufacturer in order to inform future system development. It is likely that the transmission of data will be between the C-UAS system and a server operated by the manufacturer or a manufacturer-instructed third party. It may require the legitimate passage of data from the C-UAS system to the server, however there may be a number of additional data transfers occurring in the background of which the user is not aware.

There are two elements of potential concern regarding the data stored and transferred to remote servers by a C-UAS system.

Firstly, the transmission of any data to a trusted second party has the potential to be intercepted by a malicious third party either during the process of transmission or once stored at a remote location.

Secondly, there is the possibility that the second party (the C-UAS manufacturer) is actively sharing the data with a third party without the knowledge of the C-UAS system user. This may be conducted in accordance with the terms and conditions signed at the point of installing the C-UAS software and/or in accordance with domestic laws of the manufacturer, some countries have broad powers requiring companies to share data held in that country with the state (including their intelligence services).

The approach to reducing the vulnerabilities depends largely on how the C-UAS system will be used and the environment that it is to be deployed in. A C-UAS system used where user identity is sensitive and/or data sensitivity is of the highest level, may require additional mitigation measures to be implemented, or an alternative C-UAS system to be chosen. It is therefore recommended that the Cyber Assessment Framework (CAF)[2] is used to establish the level of risk to the system and from that the measures required to protect the system that will then need to be included within the technical OR.

Prioritising the requirements

This process will identify a number of site-specific technical requirements. A key part of this process is prioritising the importance of each specific requirement. This is necessary as it is unlikely that the available solutions will be able to fully deliver against every specified requirement. Therefore, as the OR is being developed, the importance of each requirement should be rated.

It is recommended that the same MoSCoW (MUST, SHOULD, COULD or WON'T) scoring metrics be used to rate the criticality of the requirements, as has been used within the NPSA C-UAS Standard.

The information in the OR may be sensitive as it will contain detailed information in relation to the site's vulnerability to C-UAS threats. As it is completed it is important to consider who will need to have sight of it and therefore the protective marking that the completed document should be given, and how to enable access to those that require it. The content of the OR should be validated before the information is developed into a specification.

[2] For more information on the CAF visit the National Cyber Security Centre website

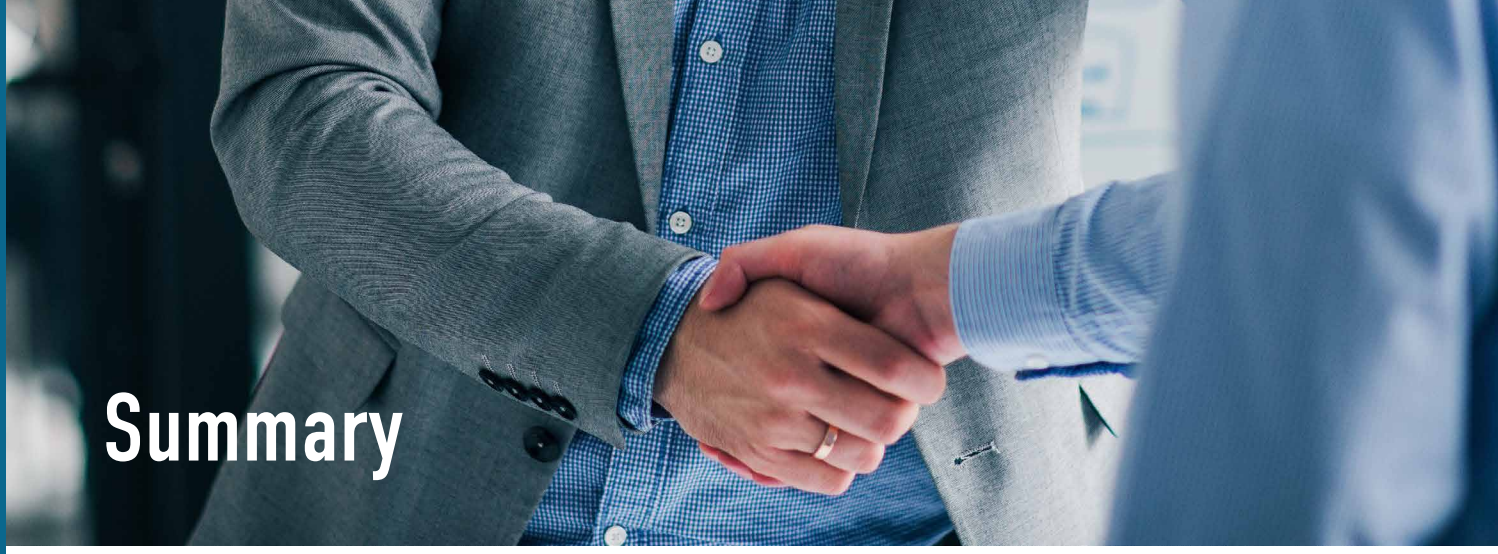
How Should The OR Be Used?

Once the OR has been completed, it should be converted into a detailed technical requirement for C-UAS DTI technology. This will likely need to be done in conjunction with subject matter experts working within this subject area. The technical requirement should be used to inform the selection of appropriate technology as part of any procurement process. Guidance as to how this should be done is provided in the NPSA guidance document titled Countering Threats From Uncrewed Aerial Systems - A guide to using the CSE and Selecting Evaluated Products, which provides advice to sites on how to use the results listed in the NPSA Catalogue of Security Equipment (CSE). The requirements should be matched to the C-UAS standard and the equipment listed within the CSE and used to inform the down selection of technology as part of the procurement process.

The development of the technical requirements is a complex task and detailed engagement will be required with those that have prepared the OR and those responsible for preparing the technical requirement. This technical document will need to set out the very detailed information that will be taken into the specification. This will include making sure that the requirements that are defined deliver the desired effect.

As the design and delivery of a technical solution develops it will be very important to make sure that if the requirements cannot be met this is fed back to the originators. This may be because it is simply too expensive to deliver a particular element of the requirement or that it is technically not possible to do. All variations to the requirements must be fully traceable and their impact understood.

Finally, the content of the OR should be approved at a suitable level within the site's senior leadership. Agreement should be sought that the content reflects the site's needs and that the organisation is willing to progress to the next step in developing the C-UAS technical solution.



Summary

The process that has been set out in this guidance document is intended to enable those responsible for developing C-UAS technology to:

- Understand the benefits and steps involved in the OR process.
- Gather the information required to complete the OR.
- Answer the OR questions.
- Understand how the information can now be used to inform the procurement and design process.
- Consider the legal implications associated with deploying and using any C-UAS technology

The process has been developed to reduce the risk of sites purchasing equipment that does not perform to the level required, meet the specific requirements of the site or simply does not provide the right level of risk mitigation.

The C-UAS guidance is being updated on a regular basis and the C-UAS equipment that is available is continually evolving. Before commencing detailed planning, the Extranet should be checked and advice should also be sought from a NPSA adviser to make certain the most up to date advice is available.

Annex A – requirements questions

Prior to completing the OR, users should ensure that they are familiar with the NPSA guidance Countering The Threats From Uncrewed Aerial Systems – A Guide To Using The CSE And Selecting Evaluated products, and the terms and definitions contained within. This includes but isn't limited to Threat and Protection Tiers.

	Question	Requirement	Level of importance Must, Should, Could, Won't	Comment
	THE THREAT			
1	Which assets have been identified as being more vulnerable to a UAS threat?			To be identified through a completed VA.
2	Which threat scenarios have been identified as being of most concern?			To be identified through a completed VA.
3	Does the C-UAS system need to address security and/or safety risks?			The development of the overarching C-UAS strategy and associated plan will define the bounds of the project, and identify whether it is to address either security and/or safety risks
4	Based on items 1,2 and 3, which Threat Protection Tier is required of the system?			To be identified through a completed VA and understanding of the NPSA detect, track and identify standard.

	Question	Requirement	Level of importance Must, Should, Could, Won't	Comment
	OPERATIONAL NEEDS			
5	What do you need to be able to detect: a) UAV? b) Ground control station? c) Both			The answer should be informed by the **VA and the intended operational response** associated with each threat scenario. For example, if the threat scenario is protestors causing disruption to their site and their primary emphasis is on arresting/engaging the pilot then the organisation may consider detection of the GCS to be of paramount importance. If, however, the threat scenario is a terrorist delivering a payload on their site then the organisation may decide that detection of the UAV is of the upmost importance. N.B. The NPSA standard requires detection of both the UAV and GCS at Threat Levels 3 and 4.
6	How many UAVs and/or GCS do you require the system to be able to detect simultaneously?			The answer for this should come directly from your site's completed VA and will be dependent on the threats faced by your site. N.B. The NPSA standard requires the system to be able to detect at least 1 UAV and/or GCS at Threat Levels 1 and 2, at least 2 UAVs and/or GCS at Threat Level 3, and at least 3 UAVs and/or GCS at Threat Level 4.
7	Is tracking required (i.e. locate and follow) of: a. UAV b. Ground control station c. Neither d. Both?			This will be informed by the operational response plans in place. As identified in relation to detection both the VA and Response Plan will determine if and what tracking is required. The response plan will consider the most likely scenarios and set out the appropriate response. Being able to track the movement of the GCS may assist in deploying security officers or police to the pilot.

	Question	Requirement	Level of importance Must, Should, Could, Won't	Comment
8	If yes, how many UAVs and/ or GCS do you require the system to be able to track simultaneously?			To be identified through a completed **VA**. If the system has tracking capability, the NPSA standard requires the system to be able to track at least 1 UAV and/or GCS at Threat Levels 1 and 2, at least 2 UAVs and/or GCS at Threat Level 3, and at least 3 UAVs and/or GCS at Threat Level 4.
9	Is UAS identification required, i.e. further information about the size and type of UAS?			The answer for this should come directly from your site's completed **VA** and will be dependent on the threats faced by your site. It will also be informed by the site specific **response plan** to ensure that any response is proportionate to the threats faced. The size of the UAS, defined as micro, small, medium or large will be identified through the **VA**. The NPSA standard requires tracking of the UAV at Threat Level 3 and tracking of both the UAV and GCS at Threat Levels 4, and identification of both the UAS at Threat Levels 3 and 4. Therefore all systems listed in the NPSA CSE at Protection Tier 3 will have the ability to track and identify a UAV, and all systems listed at Protection Tier 4 will have the ability to track a UAV and GCS and identify a UAS.
10	If yes, how many UAVs and/ or GCS do you require the system to be able to identify simultaneously?			This is determined through the **VA**. If the system has identification capability, the NPSA standard requires the system to be able to identify at least 1 UAV and/or GCS at Threat Levels 1 and 2, at least 2 UAVs and/or GCS at Threat Level 3, and at least 3 UAVs and/or GCS at Threat Level 4.

	Question	Requirement	Level of importance Must, Should, Could, Won't	Comment
11	How far away should the system be able to detect out to, and subsequently what is the area of coverage required?			The **VA** should be used to inform this, through identifying the key assets to be protected and the most likely threat scenarios (including the identification of likely launch sites and associated flight paths). Additionally, outlining the protection offered by existing mitigations will assist in identifying where there are potential 'blind spots', for example, in CCTV coverage, and furthermore identifying areas which are most vulnerable to UAS threats.
12	What is an acceptable false alarm rate?			This should be informed by the **response plans** and the **risk assessment** in place at a site. The higher the risk and the fuller the response the less appetite there is likely to be for false alarms. The NPSA standard categorises false alarm rate as LOW, i.e. an average of 0-3 false alarms per 24hrs, MEDIUM, i.e. an average of 3.1 to 12 false alarms per 24 hrs, and HIGH, i.e. an average of greater than 12 false alarms per 24hrs
13	What other technology does the C-UAS system need to be able to integrate with?			The **strategy and response plan** may inform the level of integration with other technology and security management systems. The NPSA standard states that the C-UAS system COULD allow for interoperability with established security management systems at Threat Levels 1 and 2, and SHOULD allow for interoperability with established security management systems at Threat Levels 3 and 4.

	Question	Requirement	Level of importance Must, Should, Could, Won't	Comment
14	Where should the information gathered be relayed to?			To be informed by the site command and control arrangements and the C-UAS response plan. Is the information only required in the Site Security Control Room or is it required on a hand held device as well for a security officer to act on?
15	What information should the system record and store, how long should it be stored and how should it be extracted?			The information obtained in relation to any activation of the equipment may need to be recovered to support the investigation of any offences or the review of the handling of the incident. The police may also need to extract information to support their investigation or provide evidence to a potential prosecution.
	ENVIRONMENTAL FEATURES			
16	Under what weather conditions should the C-UAS system be able to operate?			This will be identified through knowledge of the local **operating environment**. This should stipulate the extremes of temperature, wind speed, humidity, precipitation and cloud cover that can be expected.
17	Does the C-UAS system need to be able to operate in a rural and/or urban environment?			This will be identified through knowledge of the local **operating environment**. The overall site C-UAS strategy and associated plan should define the site's operating environment. This may be assisted by results from the vulnerability assessment process.
18	Are there any technologies on or surrounding the site which could be impacted by the installation and use of C-UAS DTI technology? If so, define.			This will be identified through knowledge of the local operating environment. For example, the installation of an active radar may impact on other technology operating in the same frequency band.

	Question	Requirement	Level of importance Must, Should, Could, Won't	Comment
19	Are there any technologies on or surrounding the site which could impact the installation and use of C-UAS DTI technology? If so, define.			This will be identified through knowledge of the local **operating environment**. For example, technology operating in the same frequency band as some RF technology may impact on its use.
20	What other environmental issues do you need to consider?			Examples of environmental issues include: ■ Topography, causing line of sight issues ■ Large buildings/features, water, vegetation that may interfere with radio waves ■ Presence of transmitters ■ Identification of equipment that may be interfered with by certain type of DTI system (e.g. radar) ■ Off-site locations where privacy may be an issue and steps taken (e.g. long-range cameras)
	THROUGH LIFE SUPPORT			
21	What is the required lifespan of the C-UAS system?			This may be influenced by factors such as the envisaged lifespan of the site, threats and associated mitigations. This information should be identified through the strategy and plan. It may also be impacted by aspects such as the availability of hardware and software updates, and expansion capability.

	Question	Requirement	Level of importance Must, Should, Could, Won't	Comment
	SECURITY AND LEGAL			
22	What consideration needs to be given to the security of the system during both installation and live operations?			The **CAF** should be completed to understand the level of risk and the mitigation required.
23	Is your site exposed to an espionage threat and if so what are your requirements of C-UAS technology?			Should certain technologies, types of connectivity or supplier groups be excluded as technology is being selected.
24	What other security requirements for the system need to be identified during both installation and operation?			A security risk assessment should identify areas of concern.
25	What legislation does the C-UAS system need to comply with and how will you ensure its compliance?			Guidance should be sort from the site's legal team to identify requirements that may be relevant to each specific site and technology being considered.
26	What technologies are you not permitted to operate, due to legal or environmental considerations?			Guidance should be sort from the site's legal team to identify requirements that may be relevant to each specific site and technology being considered.

Annex B – Glossary of terms

Catalogue of Security Equipment (CSE)	A catalogue of equipment that has been assessed by NPSA and proven to meet the necessary requirements to provide utility to the NPSA user
Counter-Uncrewed aerial system (C-UAS)	A range of measures to combat suspected hostile UAS activity
Detection	The function of a C-UAS system to sense and classify the presence of a UAS
Distracted operator	An operator of the C-UAS system who has to concurrently perform other non C-UAS related tasks
Fixed wing UAV	Consists of a rigid wing that generates lift and forward air speed
Ground control station (GCS)	The ground-based control element of the uncrewed aircraft system used by the human operator of the uncrewed aircraft
Identification	The Capability of a C-UAS system to support the determination of the size and type of UAV or UAS either automatically or via manual operator inspection
Operational requirement	A structured process for outlining and assessing security risks and identifying suitable risk mitigation options
Rotary wing UAV	A UAV that derives its lift from one or more rotary wings
Uncrewed aerial system (UAS)	Consists of a UAV, GCS and the control link between the two
Uncrewed aerial vehicle (UAV)	Also referred to as drone, remotely piloted aircraft or uncrewed air vehicle, which is the aerial vehicle element of a UAS